REMARKS

This Amendment is fully responsive to the non-final Office Action dated September 29, 2008, issued in connection with the above-identified application. A petition for a one-month extension of time accompanies this Amendment. Claims 16-27 were previously pending in the present application. With this Amendment, claims 16-23, 25 and 26 have been amended; and claim 27 has been canceled without prejudice or disclaimer to the subject matter therein. Accordingly, claims 16-26 are all the claims now pending in the present application. No new matter has been introduced by the amendments made to the claims. Favorable reconsideration is respectfully requested.

The present application is being examined under the patent prosecution highway (PPH) program. The Applicants maintain that claims 16-26 (as amended) sufficiently correspond to the allowable/patentable claims in corresponding application JP 2006-519466 filed in Japan on December 20, 2007. The Applicants note the following correspondence between the allowable/patentable claims of JP 2006-519466 and claims 16-26 of the present application:

JPO Application	Present Application
1	16
2	17
3	18
4	19
5	20
6	21
7	22
8	23
9	24
10	25
12	26

To facilitate the Examiner's reconsideration of the application, the Applicants have provided amendments to the specification and the abstract. The changes to the specification and the abstract include minor editorial and clarifying changes. Replacement paragraphs and a new abstract are enclosed. No new matter has been introduced by the amendments made to the specification and the abstract.

In the Office Action, claims 16-27 have been rejected under 35 U.S.C. 103(a) as being unpatentable over Marshall et al. (U.S. Patent No. 4,933,969, hereafter "Marshall").

As noted above, claim 27 has been canceled thereby rending the above rejection to that claim moot. Additionally, the Applicants have amended independent claims 16, 25 and 26 to help further distinguish the present invention from the cited prior art. For example, claim 16 (as amended) recites the following features:

"[a] data processing device for playing back a digital work recorded on a recording medium having also recorded thereon (i) a plurality of record digest values generated from a plurality of data blocks constituting the digital work and (ii) record signature data generated by applying, with use of a signature key, a signature generating algorithm to a first combination made of some or all of the plurality of record digest values, the data processing device comprising:

a verification key storing unit configured to store a verification key corresponding to the signature key;

a using unit configured to play back the digital work;

a selecting unit configured to, each time the digital work is played back, randomly select a predetermined number of data blocks from all of the plurality of data blocks, the predetermined number being smaller than the number of all the plurality of data blocks;

a calculating unit configured to calculate a plurality of calculation digest values from the selected data blocks;

a reading unit configured to read remaining record digest values corresponding to unselected data blocks from among the plurality of record digest values;

a generating unit configured to generate a second combination based on calculation digest values and the remaining record digest values, the second combination being the same as data which is generated from the first combination by replacing record digest values corresponding to the selected data blocks with corresponding calculation digest values;

a signature verifying unit configured to verify the record signature data by applying, with use of the verification key, a signature verification algorithm to the second combination and the record signature data; and

a use controlling unit configured to stop said using unit from playing back the digital work when the verification is unsuccessful." (Emphasis added).

12

The features emphasized above in independent claim 16 are similarly recited in independent claims 25 and 26 (as amended). Specifically, claims 25 and 26 are directed respectively to methods that include steps having similar features of the selecting unit and verifying unit recited in claim 16. The features emphasized above are also fully supported by the Applicants' disclosure (see e.g., Fig. 17; Fig. 18; pgs. 38-40; and Fig. 54(step S4057).

The present invention (recited in independent claim 16, and similarly recited in independent claims 25 and 26) is distinguishable over the cited prior art in that a selecting unit is operable to, each time the digital work is used, randomly select a predetermined number of data blocks from all of the plurality of data blocks constituting the digital work. Additionally, a signature verifying unit is operable to verify the record signature data by applying, with use of the verification key, a signature verification algorithm to a second combination and the record signature data.

With this structure, data blocks from which calculation digest values are calculated are randomly selected from all of the plurality of data blocks constituting the digital work, each time the digital work is played back regardless of a user's wish. Also, the record signature data is verified with use of the second combination generated based on the selected data blocks. By selecting a predetermined number of data blocks and performing verification with use of the selected data blocks, the present invention provides the advantageous effect of reducing the processing load for each verification.

Furthermore, as the data blocks are randomly selected, an unauthorized third person cannot easily estimate which one(s) of the plurality of data blocks is selected. In addition, as the selecting unit selects the data blocks regardless of the user's wish, the user cannot intentionally prevent certain data blocks from being selected. It is therefore possible to prevent fraudulent acts involving falsification of unselected data blocks.

Moreover, once the selecting unit randomly selects the data blocks from all of the plurality of data blocks each time the digital work is played back, the verifying unit verifies the record signature data based on the data blocks selected each time the digital work is played back. Consequently, as the playback is repeated, all of the data blocks are expected to be selected as data blocks from which the calculation digest values are calculated. Hence, even if

13

certain data blocks were falsified, such falsification can be detected.

In the Office Action, the Examiner relies on Marshall for rendering obvious the features recited in independent claims 16, 25 and 26. However, the Applicants assert that Marshall fails to render obvious the features recited in at least independent claims 16, 25 and 26, as amended.

Specifically, Marshall discloses a system for re-calculating a global MAC in order to check the integrity of the whole file set (the digital work of the present application), and for comparing the re-calculated global MAC with another global MAC (the record signature data of the present application) that was calculated before. In particular, Marshall discloses that "the global MAC is still calculated from the individual MAC's of the messages, albeit indirectly, and validates the whole of the information-all messages of all blocks" (see col. 2, lines 42-46). Additionally, Marshall discloses that "[i]f the integrity of the whole set of files is to be checked, then the global MAC of the MAC's in the directory 112 is calculated, and compared with the stored global MAC in register 115 by the MAC comparator 44 (FIG. 2) in the security module 16."

Thus, in Marshall, in order to verify the whole file set, each MAC value is calculated for a different one of all of a plurality of messages (i.e., the data blocks of the present application), and a global MAC is re-calculated with use of the MAC values. In other words, the system disclosed in Marshall neither discloses nor suggests the structure of selecting a predetermined number of blocks and performing verification based on the selected blocks, as in the present invention.

Based on the above discussion, one clear problem with the system disclosed in Marshall is that as each MAC value needs to be re-calculated for a different one of all of a plurality of messages, the processing load for each verification is large. In contrast, the present invention includes a selecting unit and the verifying unit, and limits the number of selected data blocks, from which the calculation digest values are calculated, to a predetermined number. This way, the load for every verification processing can be reduced.

In addition, in the present invention, the selecting unit randomly selects a predetermined number of data blocks each time the digital work is played back, and the

14

verifying unit performs verification based on the selected data blocks. This way, the present invention has the advantageous effect of, as the playback of the digital work is repeated, further complementing degradation of verification accuracy for limiting the number of data blocks from which the calculation digest values are calculated; thereby reducing a processing load on each verification without degrading the verification accuracy.

In summary, the cited prior art fails to disclose or suggest the following features and advantageous effects of the present invention (recited in independent claim 16, and similarly recited in independent claims 25 and 26):

1) reducing a load on every verification processing by limiting the number of selected data blocks, from which the calculation digest values are calculated, to a predetermined number; and

2) complementing degradation of verification accuracy arisen from limiting the number of data blocks from which the calculation digest values are calculated, because these data blocks, from which the calculation digest values are calculated, are randomly selected each time the digital work is played back.

Accordingly, no combination with or modification of Marshall would result in, or otherwise render obvious, independent claims 16, 25 and 26 (as amended). Likewise, no combination with or modification to Marshall would result in, or otherwise render obvious, claims 17-24 at least by virtue of their dependencies from independent claim 16.

In light of the above, the Applicants respectfully submit that all the pending claims are patentable over the prior art of record. The Applicants respectfully request that the Examiner withdraw the rejections presented in the outstanding Office Action, and pass the present application to issue.

Respectfully submitted,

Masao NONAKA et al.

/Mark D. Pratt/
By: 2009.01.29 13:22:03 -05'00'
_____

Mark D. Pratt
Registration No. 45794
Attorney for Applicants

MDP/ats
Washington, D.C. 20006-1021
Telephone (202) 721-8200
Facsimile (202) 721-8250
January 29, 2009